Commission
d'accès à l'information
du Québec

# Guide d'accompagnement

## Réaliser une évaluation des facteurs relatifs à la vie privée

Document mis à jour
le 10 mars 2021

*Les informations incluses dans ce guide reflètent les lois avant leur modification par la Loi 25. Il sera révisé ultérieurement. Pour connaître les modifications apportées au régime de protection des renseignements personnels, qui entreront en vigueur en septembre 2022 et les années suivantes, nous vous invitons à consultez la section Espace évolutif - Modernisation des lois du site Web de la Commission.*

## Version de travail

Ce guide est appelé à évoluer. Il sera révisé à la lumière de l'adoption de la Loi 25, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels.* Il pourrait être remanié en profondeur.

La Commission vous invite tout de même à lui adresser tout commentaire ou suggestion. Veuillez les faire parvenir à l'adresse courriel suivante : veille@cai.gouv.qc.ca

# INTRODUCTION

## Le droit à la vie privée est un droit fondamental

Il est protégé par la *Charte des droits et libertés de la personne*[1]. Pour toute organisation[2], qu'elle soit entreprise du secteur privé ou organisme public, ce droit se traduit dans l'obligation de respecter l'intimité et la vie personnelle des personnes en minimisant les renseignements personnels qu'elle recueille, utilise, communique et conserve et dans l'obligation d'en assurer la confidentialité.

## Le rythme effréné de l'innovation commande la vigilance.

Les normes et la législation peinent à suivre l'émergence continue et accélérée des nouvelles technologies. Leur adoption devient souvent un préalable à la rentabilité et à la survie des organisations. L'information, incluant les renseignements personnels, est une ressource de plus en plus prisée. Les technologies facilitent la collecte, le traitement et le stockage de renseignements personnels et peuvent impacter la vie privée des personnes.

## La protection de la vie privée nous concerne tous.

À l'ère numérique, la responsabilité de veiller au respect de la vie privée ne repose plus seulement sur les épaules des institutions ou des citoyens. Elle incombe désormais à toutes les organisations, publiques comme privées.

Celles qui l'ont compris et qui agissent en conséquence diminuent leur chance de causer des préjudices aux personnes et d'avoir à gérer les contrecoups de ces problèmes (par exemple, des recours juridiques, offrir des compensations financières, des atteintes à la réputation de votre organisation, etc.). Elles sont aussi mieux perçues par le public et par les investisseurs[3].

---

[1] RLRQ, c. C-12, art. 5.

[2] Dans ce guide, les parties où le terme « organisation » est utilisé s'appliquent autant aux entreprises du secteur privé qu'aux organismes du secteur public. Le texte sera spécifique lorsque qu'il s'appliquera uniquement à l'un ou l'autre des secteurs.

[3] En 2018, **91 % des Québécois** accordaient de l'importance à la protection de leurs renseignements personnels et auraient fait davantage affaire avec une entreprise possédant une bonne réputation en la matière (sondage Léger Marketing réalisé pour la CAI) : https://www.cai.gouv.qc.ca/documents/CAI_Sondage_perception_2018.pdf)

Le processus dont il est question dans ce guide est donc non seulement un moyen de mener à bien une évaluation des facteurs relatifs à la vie privée, mais aussi l'occasion de démontrer que votre organisation se préoccupe de ces enjeux.

## Ce guide a été conçu par la Commission d'accès à l'information du Québec (CAI).

La CAI veille à la promotion et au respect des droits des citoyens en ce qui concerne l'accès aux documents des organismes publics et la protection de leurs renseignements personnels[4].

Elle veille aussi au respect des lois :

- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels[5] (Loi sur l'accès);
- La Loi sur la protection des renseignements personnels dans le secteur privé[6] (Loi sur le privé).

L'équipe de la CAI est à votre disposition pour répondre à vos questions générales concernant le présent guide. Elle ne donnera toutefois pas d'avis ou de conseils concernant l'analyse et l'évaluation des facteurs relatifs à la vie privée (EFVP) d'un projet particulier.



[4] Pour plus d'information, consultez le site Internet de la CAI : **www.cai.gouv.qc.ca**.
[5] RLRQ, c. A-2.1.
[6] RLRQ, c. P-39.1.

# QUEL EST L'OBJECTIF DE CE GUIDE?

**Ce guide a pour objectif de vous accompagner dans l'évaluation des risques liés à la vie privée** si vous devez concevoir, développer ou exploiter :

- Un projet[7] ou une initiative impliquant des renseignements personnels[8];
- Un projet risquant d'avoir une incidence sur le respect de la vie privée des personnes.

**Exemples de projets concernés pouvant impliquer la collecte, l'utilisation ou la communication des renseignements personnels :**

- Développer un nouveau système d'information ou une technique de personnalisation d'un produit ou d'un service;
- Chercher une nouvelle clientèle, explorer de nouveaux marchés;
- Faire appel à un système d'algorithme ou d'intelligence artificielle;
- Installer un système de vidéosurveillance;
- Comparer différentes versions de bases de données ou de fichiers;
- Acquérir ou fusionner des organisations;
- Utiliser des empreintes digitales, la géolocalisation, un système de reconnaissance faciale, des objets connectés, des capteurs pour villes intelligentes, etc.

---

[7] Le terme **projet** réfère à toute activité au sein d'une organisation : mise en place ou modification d'un programme ou d'un service, recours à une technologie particulière, initiative publique, etc.

[8] Les **renseignements personnels** sont ceux qui concernent une personne physique et permettent de l'identifier (art. 54 de la Loi sur l'Accès et art. 2 de la Loi sur le privé). Sauf exception, ils sont confidentiels. Cette définition est la même pour les organisations publiques que pour les organisations privées, quel que soit le support ou le format (écrit, graphique, sonore, visuel, informatisé ou autre).

# À QUI S'ADRESSE CE GUIDE?

À toute personne responsable de la conception, du développement ou de l'exploitation de projets au sein d'une organisation.

**Principales personnes concernées :** les responsables de la protection des renseignements personnels

**Autres exemples de personnes impliquées :**

- **Dans les petites entreprises du secteur privé**[9] **:** chefs d'entreprise, commerçants, artisans, travailleurs autonomes, responsables associatifs, etc.;
- **Dans les grandes entreprises privées :** responsables des affaires juridiques, responsables organisationnels de la gestion de risque, toute personne chargée de la sécurité des systèmes d'information, de l'éthique, de la gestion documentaire, etc.;
- **Dans les organisations du secteur public**[10] **:** responsables organisationnels de la sécurité de l'information (ROSI), responsables de la gestion documentaire (RGD), responsables de l'éthique (RE), responsables du développement ou de l'acquisition des systèmes d'information (RDASI), responsables de l'architecture de sécurité de l'information (RASI), responsables de la continuité des services (RCS), responsables de la gestion des technologies de l'information (RGTI), responsables de la sécurité physique (RSP), responsables organisationnels de la gestion de risque, responsables de la vérification interne (RVI), etc.

---

[9] Le terme **entreprise** réfère à l'exercice, par une ou plusieurs personnes, d'une activité économique organisée, qu'elle soit ou non à caractère commercial, consistant dans la production ou la réalisation de biens, leur administration ou leur aliénation, ou dans la prestation de services (art. 1525 du *Code civil du Québec* (CCQ-1991)). Cette définition s'étend notamment à l'entreprise individuelle (travailleur autonome), à la société par actions (compagnie), à la société en nom collectif (S.E.N.C.), à la société en commandite (S.E.C.), à la société en participation, à la personne morale sans but lucratif, au syndicat de copropriété, à l'association (p. ex. : syndicat), au groupement de personnes (p. ex. : consortium) ou à une fiducie exploitant une entreprise à caractère commercial.

[10] L'intitulé du poste peut varier.

# QU'EST-CE QU'UNE ÉVALUATION DES FACTEURS DE RELATIFS À LA VIE PRIVÉE (EFVP)?

**Un processus préventif**

L'EFVP[11] est une démarche préventive visant à mieux protéger les renseignements personnels et à mieux respecter la vie privée des personnes physiques.

Elle consiste à considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées.

**Ces facteurs sont**

- La conformité de votre projet à la législation applicable à la protection des renseignements personnels et le respect des principes qui l'appuient;
- L'identification des risques d'atteinte à la vie privée engendrés par votre projet et l'évaluation de leurs impacts;
- La mise en place de stratégies pour éviter ces risques ou les réduire efficacement.

Ce processus vise **d'abord** à protéger les personnes physiques concernées par ces renseignements. Il vise **aussi** la mise en place de mesures adéquates pour respecter vos obligations en matière de protection des renseignements personnels. Ainsi, l'EFVP permet d'éviter des problèmes que causerait une gestion inadéquate (plaintes, incidents de sécurité, poursuites judiciaires, atteinte à l'image, etc.).

**Une bonne pratique évolutive**

Dès que des renseignements personnels ou la vie privée des personnes sont concernés, réaliser une l'EFVP constitue une bonne pratique. Cependant, l'EFVP n'est efficace que si elle évolue de façon continue : elle doit être revue au besoin, tout au long de la vie du projet.

---

[11] En anglais, l'EFVP est connue sous l'expression *Privacy Impact Assessment* (PIA).

# TABLE DES MATIÈRES

**1. Préparer votre évaluation des facteurs relatifs à la vie privée ..... 1**
1.1. Vous poser les bonnes questions avant de commencer ..... 1
1.2. Définir votre projet ..... 3
1.3. Établir le partage des rôles et des responsabilités ..... 5
1.4. Connaître vos obligations en matière de protection des renseignements personnels ..... 5
1.5. Repérer les renseignements personnels impliqués dans votre projet ..... 8
1.6. Identifier les points où votre organisation entre en interaction avec les renseignements personnels ..... 10
**2. Analyser et évaluer les facteurs relatifs à la vie privée ..... 12**
2.1. Respecter les obligations et les principes de protection des renseignements personnels ..... 12
2.2. Repérer et décrire les risques sur la vie privée engendrés par votre projet ..... 15
2.3. Évaluer l'impact des risques identifiés ..... 19
2.4. Éliminer ou réduire les risques d'atteintes à la vie privée ..... 21
2.5. Faire le suivi de l'évaluation des facteurs relatifs à la vie privée ..... 23
**3. Rédiger un rapport d'évaluation ..... 24**
3.1. À quoi sert le rapport? ..... 24
3.2. Rédiger un rapport est-il obligatoire? ..... 24
3.3. Que devrait contenir le rapport? ..... 25

**À COMPLÉTER**

**Vous rencontrerez ce symbole au cours de votre lecture.**
**Chacune de ses apparitions est une invitation à produire une section en vue de votre rapport d'EFVP.**

# 1. PRÉPARER VOTRE ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

La première étape d'une EFVP consiste à vous poser les bonnes questions et à bien comprendre quels aspects de votre projet sont concernés.

## 1.1. Vous poser les bonnes questions avant de commencer

### Êtes-vous obligé de faire une EFVP?

Faire une EFVP n'est pas obligatoire, sauf pour certains organismes publics (voir section 3.2 *Rédiger un rapport est-il obligatoire?*). Mais si votre projet implique la collecte, l'utilisation ou la communication de renseignements personnels, une EFVP est fortement recommandée.

Ne concluez pas trop rapidement qu'une EFVP est superflue sous prétexte que vous ne pensez pas utiliser de renseignements personnels. Des renseignements en apparence anodins peuvent, une fois croisés avec d'autres, révéler de l'information sur les personnes concernées.

En outre, un survol de votre projet pourrait révéler des enjeux insoupçonnés sur la vie privée des personnes visées par celui-ci..

Si vous décidez de ne pas réaliser d'EFVP, soyez en mesure d'expliquer et de justifier pourquoi vous ne le faites pas.

Si des changements sont apportés à un projet, vérifiez d'abord si une EFVP a déjà été faite et révisez-la pour rendre compte de ces changements.

### Quand faire l'évaluation?

Vous devez commencer votre EFVP **au tout début de votre projet** plutôt qu'en fin de parcours :

- Pour pouvoir influencer son déroulement en cours de route
- Pour agir et choisir la solution qui protège et respecte le mieux la vie privée

Pour les projets de grande envergure, vous pouvez faire une EFVP préliminaire, plus courte et moins exhaustive, avant une EFVP complète.

Par exemple, certains projets requièrent des études d'opportunité, de préfaisabilité ou de faisabilité. Une EFVP préliminaire dans le cadre de ces études peut éviter d'engager des

frais pour des solutions qui pourraient s'avérer non conformes ou engendrer des enjeux disproportionnés pour les personnes par rapport à vos objectifs d'affaires.

## Qu'allez-vous inclure dans votre évaluation?

Vous avez intérêt à délimiter clairement la portée de votre évaluation et à tenir votre analyse à un niveau adapté à votre projet.

**Exemple 1 :** Vous décidez de ne pas inclure la révision des procédures d'identification des personnes dans votre projet d'assistant virtuel en ligne. Vous jugez que cela n'a pas d'importance, car votre système actuel fonctionne bien avec votre service à la clientèle en personne et au téléphone. **Votre portée est peut-être trop étroite.** Des éléments importants pourraient manquer à votre évaluation, car une identification en ligne n'a peut-être pas les mêmes caractéristiques qu'une identification en personne ou au téléphone.

**Exemple 2 :** Pour le même projet, vous décidez finalement de revoir les procédures d'identification, l'hébergement des données de vos clients, les formulaires de confidentialité de vos employés du service à la clientèle et l'ensemble de vos infrastructures systèmes. **Votre portée est sans doute trop large.** Des évaluations distinctes pourraient sans doute être produites pour certains sous-processus.

**Exemple 3 :** Pour le même projet, vous ne faites que la révision de vos politiques et directives de service à la clientèle, sans vous attarder aux détails techniques de la solution logicielle que vous avez acquise ni aux procédures d'identification des personnes. **Votre analyse se situe peut-être à un trop haut niveau.** Vous manquerez sans doute des éléments importants qui existent au niveau de la solution logicielle ou des procédures d'identification.

En définissant clairement votre portée, vous aurez une meilleure idée des ressources à impliquer dans la réalisation de l'EFVP.

Vous devez être en mesure de justifier les limites que vous imposez à votre évaluation.

**Exemple 4 :** Pour le même projet, des EFVP distinctes ont récemment été produites par votre organisation concernant les procédures et les processus d'identification des personnes qui s'adressent au service à la clientèle. **Vous décidez de ne pas refaire cette partie d'analyse et vous analysez uniquement la partie qui s'ajoute concernant l'identification par l'assistant virtuel.** Vous l'indiquez clairement dans votre rapport afin d'informer les gens des limites que vous posez à votre évaluation.

### Qui devriez-vous impliquer?

**Principalement**

- Les personnes responsables du projet;
- Les personnes au courant des bonnes pratiques en matière de respect de la vie privée, de protection des renseignements personnels et de sécurité de l'information;
- Les personnes responsables des affaires juridiques;
- Les autorités compétentes de votre organisation devant prendre position sur la gestion des risques à la fin de la démarche (voir section 3*)*.

**Selon l'envergure du projet ou les impacts sur la vie privée**

- Vos collègues de travail dans certains départements : ressources humaines, gestion de risques, gestion documentaire, affaires juridiques, relations avec la clientèle, etc.;
- Vos clients, partenaires corporatifs, sous-traitants, etc.

### Devez-vous documenter votre démarche?

**Vous avez tout avantage à le faire.** Conservez une trace écrite de toute votre démarche.

En cas de problème ou de question en lien avec la vie privée ou avec la protection des renseignements personnels, votre documentation attestera du sérieux de votre réflexion.

## 1.2. Définir votre projet

Cette première étape de l'EFVP est surtout descriptive. L'objectif est de documenter les informations importantes pour vous permettre d'évaluer les risques et les moyens d'éliminer ou de réduire ces risques (voir sections 2.2, 2.3 et 2.4).

### Présentez les grandes lignes de votre projet

- En quoi consiste-t-il?
- Quel était le contexte quand l'idée de ce projet est apparue?
- Quelle est/était la situation au moment de son lancement?
- Quel est l'échéancier de sa mise en œuvre?

## Expliquez quels sont les objectifs qui motivent votre projet

Ces objectifs peuvent expliquer pourquoi vous devez mettre en place de nouvelles mesures ou pratiques impliquant la gestion des renseignements personnels.

Cet objectif doit être **légitime** et se rapporter à des **préoccupations réelles et justifiables**.

**Exemples** d'objectifs visés par un projet :

- Vouloir mieux connaître votre clientèle;
- Offrir un nouveau service public;
- Déployer sur le Web un service existant;
- Accroître la sécurité d'une installation;
- Contrer la fraude;
- Vous mettre en conformité avec la réglementation;
- Conserver votre compétitivité;
- Lancer une nouvelle branche d'affaires ou rechercher une nouvelle clientèle pour appuyer votre croissance;
- Offrir une expérience client plus agréable, plus intuitive et plus efficace en créant la nouvelle version d'une plateforme.

## Privilégiez une solution proportionnée à vos objectifs et aux risques d'atteinte à la vie privée

L'évaluation de la proportionnalité doit être faite tout au long de l'évaluation des facteurs à la vie privée et de la mise en place de votre projet.

Votre solution sera proportionnelle si :

- Il existe un lien rationnel entre vos objectifs et la solution proposée, c'est-à-dire qu'il s'agit d'un moyen efficace d'atteindre l'objectif visé. Cette efficacité doit être basée sur des données concrètes et probantes;
- Que l'atteinte à la vie privée est minimale ou qu'il n'y a pas d'autres solutions efficaces moins intrusives;
- Que les avantages concrets surpassent les conséquences ou les préjudices pour les personnes concernées.

## 1.3. Établir le partage des rôles et des responsabilités

### Identifiez les parties impliquées dans le projet

- Qui sont les intervenants au sein de votre organisation
- Quels sont leurs rôles et leurs responsabilité (en incluant les responsables de la protection des renseignements personnels et de la sécurité de l'information);
- Qui sont les intervenants extérieurs (par **exemple**, vos fournisseurs de services, vos partenaires, autres organisations que vous impliquées[12], etc.);
- Qui seront les utilisateurs de votre service et quelle clientèle sera impactée.

**À COMPLÉTER**

- Description du projet
- Description des rôles et responsabilités

## 1.4. Connaître vos obligations en matière de protection des renseignements personnels

Les obligations peuvent provenir de sources différentes. Cela dépend de la nature et de l'envergure de votre projet.

Identifier vos obligations et comprendre les enjeux qu'elles impliquent n'est pas une tâche facile. En cas de doute, **n'hésitez pas à consulter un juriste**.

### Sur le plan provincial

Au Québec, l'utilisation de renseignements personnels est encadrée principalement par deux lois :

- La *Loi sur la protection des renseignements personnels dans le secteur privé*, qui s'applique aux **organisations du secteur privé** (entreprises et organismes à but non lucratif);
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, qui s'applique aux **organisations du secteur**

[12] Pour les organismes publics, pensez à mentionner les autres organisations gouvernementales, sur les plans local, provincial, fédéral et international.

**public** (ministères et organismes gouvernementaux et municipaux, organismes des réseaux de la santé et de l'éducation).

Voici une liste non exhaustive de lois qui contiennent des particularités en matière de protection des renseignements personnels :

- Code civil (RLRQ, c. CCQ-1991);
- Loi sur les archives (RLRQ, c. A-21.1);
- Loi concernant la cadre juridique des technologies de l'information (RLRQ, c. C-1.1);
- Code des professions (RLRQ, c. C-26);
- Loi sur l'administration fiscale (RLRQ, c. A-6.002);
- Code de la sécurité routière (RLRQ, c. C-24.2);
- Loi sur la protection de la jeunesse (RLRQ, c. P-34.1);
- Loi sur les services de santé et les services sociaux (RLRQ, c. S-4.2);
- Loi sur l'assurance maladie (RLRQ, c. A-29).

**Exemples** de particularités et exceptions précisées dans des lois :

- La collecte et l'utilisation du numéro de permis de conduire et du numéro d'assurance maladie sont régies par des lois, des règlements ou des directives sectorielles[13];
- La gestion du consentement est particulière pour les mineurs et les personnes majeures inaptes;
- L'utilisation et la collecte de renseignements biométriques[14] sont régies de manière spécifique et complémentaire par la *Loi concernant la cadre juridique des technologies de l'information*.

[13] Pour plus d'information sur l'utilisation des pièces d'identité, veuillez vous référez aux fiches Pièces d'identité : citoyens et Pièces d'identité : entreprises.

[14] Pour obtenir plus d'information, voir la section Biométrie du site de la Commission. Voir également note de bas de page 18.

## Sur le plan fédéral et à l'international

Le gouvernement fédéral et certaines provinces canadiennes possèdent leurs propres législations et réglementations en matière de protection des renseignements personnels. Si votre entreprise exerce ses activités dans une ou plusieurs autres provinces, assurez-vous de bien connaître les obligations qui découlent de leurs législations.

Rappelez-vous que les communications de renseignements personnels à l'extérieur du Québec et du Canada sont soumises à un encadrement particulier par les lois provinciales et fédérales.

Pour les activités à l'international, sachez que les lois peuvent différer beaucoup d'un pays à l'autre. De plus, des obligations supplémentaires pourraient s'appliquer à certaines catégories de renseignements personnels, notamment pour les renseignements sensibles.

Enfin, certaines législations ont une portée extraterritoriale. Elles s'appliquent si une organisation collecte, utilise, communique ou conserve des renseignements personnels de personnes se trouvant sur le territoire couvert par ces législations, même si cette organisation ne se trouve pas sur ce territoire, Le *Règlement général sur la protection des données* européen est un exemple. Le non-respect de ces législations s'accompagne parfois de lourdes sanctions financières.

Si vos services visent un marché ou des citoyens de l'étranger, informez-vous et considérez les impacts que ces lois pourraient avoir sur votre projet.

## Pratiques corporatives

Votre organisation peut encadrer le traitement des renseignements personnels de diverses façons : par des politiques, des processus, des procédures, des méthodes de travail, un plan et un calendrier de conservation, etc.

Bien que de tels documents internes n'aient pas force de loi, il est important d'en tenir compte dans votre évaluation pour ne pas vous écarter des pratiques en vigueur dans votre organisation. Votre travail pourrait même vous permettre d'identifier des lacunes au sein de votre organisation.

## Normes

Différentes normes internationales peuvent alimenter votre réflexion sur vos pratiques, par exemple certaines normes ISO ou la documentation produite par l'Union européenne ou l'Organisation de coopération et de développement économiques (OCDE). Consultez-les si vous cherchez à adopter les meilleures pratiques en matière de respect de la vie privée et de protection des renseignements personnels.

## 1.5. Repérer les renseignements personnels impliqués dans votre projet

### Faire l'inventaire des renseignements personnels

Afin de bien évaluer la conformité de votre projet avec la législation applicable et les risques d'atteinte à la vie privée qu'il comporte, vous devez faire l'inventaire des renseignements personnels qu'il implique. Cela vous permettra, par exemple, de vous assurerez de ne recueillir ou d'utiliser que les renseignements personnels nécessaires.

Toutefois, cette liste exhaustive n'est pas nécessaire à toutes les étapes de l'évaluation.

Par exemple, dans le rapport, une liste faisant état de regroupement de renseignements personnels de même nature pourrait suffire.

Ces regroupements contiennent des renseignements personnels qui possèdent des caractéristiques communes et/ou qui sont regroupés afin d'accomplir une fonction ou atteindre un objectif.

Votre liste doit quand même prévoir une courte énumération du contenu de ces regroupements.

**Exemples** de regroupements de renseignements personnels :

- Renseignements d'identité et coordonnées de vos clients (nom, prénom, nom d'utilisateur, mot de passe);
- Dossiers médicaux, en version électronique et papier (résultats médicaux, résumés des rencontres, données de santé, imagerie médicale);
- Dossiers d'invalidité des employés détenus par les ressources humaines (renseignements d'identité, rapports médicaux, communications avec les assureurs);
- Courriels et enregistrements téléphoniques du centre d'appels (échanges avec les clients, contenu des questions et des réponses, échantillon de la voix);
- Données de journalisation du site Internet et outil d'analyse Web (historiques des pages consultés, adresse IP, navigateur et appareil utilisé, configuration de l'affichage).

### Éléments à retenir

- Si vous n'êtes pas certain qu'un regroupement contient des renseignements personnels, conservez-le quand même dans votre liste et considérez-le dans votre EFVP.

- Incluez tous les renseignements que vous créez ou inférez sur les personnes (**exemples :** une cote de crédit, une note d'évaluation, une note dans un dossier). Ce sont des renseignements personnels.
- Pensez aux renseignements collectés automatiquement par les appareils et les systèmes informatiques que vous utilisez.
- Incluez les renseignements pseudonymisés[15], dépersonnalisés ou anonymisés[16] et agrégés[17] dans votre liste. Même si certains de ces renseignements ne sont plus directement reliés à l'identité d'une personne, les nouvelles technologies permettent bien souvent de rétablir ce lien. Il sera pertinent d'évaluer le risque de réidentification de ces renseignements.
- Même si vous ne présentez que regroupements dans le rapport d'évaluation, il est important que votre organisation soit en mesure de connaitre l'étendue de tous les renseignements personnels qu'elle détient.

## Évaluer le degré de sensibilité de ces renseignements

Un renseignement est dit « sensible », soit parce qu'il révèle quelque chose d'intime, d'unique ou si sa révélation ou son utilisation peut causer des conséquences négatives pour la personne.

La Loi sur l'accès et la Loi sur le privé reconnaissent cette distinction. Elles prévoient notamment que les mesures de sécurité soient adaptées à la sensibilité des renseignements.

**Exemples** de renseignements sensibles :

- Renseignements concernant le groupe ethnique ;
- Renseignements concernant les croyances philosophiques ou religieuses;
- Renseignements concernant la santé ou l'orientation sexuelle;
- Renseignements financiers;

[15] Des renseignements sont pseudonymisés si les informations qui identifient directement les personnes (**p. ex.** nom, prénom) sont remplacées par des informations qui les identifient de façon indirecte (**p. ex.** no de dossier).
[16] Des renseignements sont dépersonnalisés ou anonymisés s'il est impossible d'identifier une personne à partir du jeu de données. La garantie d'anonymat est obtenue à la suite de l'application d'une ou de plusieurs méthodes. L'anonymisation doit être irréversible.
[17] Des renseignements sont agrégés lorsque plusieurs données de même type sont regroupées (**p. ex.** statistiques), ce qui rend impossible l'identification d'un individu donné.

- Renseignements biométriques[18],
- Identifiants uniques[19].

## 1.6. Identifier les points où votre organisation entre en interaction avec les renseignements personnels

**Les points d'interactions peuvent être**

- Les personnes, les ensembles de personnes ou les partenaires et tiers qui accèdent aux renseignements personnels (**exemples :** employés, clientèle, sous-traitants, firmes de consultation, chercheurs externes, équipes d'entretien de bâtiments ou de systèmes informatiques, fournisseurs de télécommunication);
- Les moyens utilisés pour collecter des renseignements personnels (**exemples** : formulaires d'abonnement, boîtes courriel, messageries téléphoniques, plateformes collaboratives, sondages, questionnaires);
- Les moyens utilisés pour communiquer des renseignements personnels (**exemples :** prestations électroniques de service, échanges par courriel, service à la clientèle, sites Web, interfaces d'échange informatisées [API] ou liens électroniques sécurisés);
- Les moyens utilisés pour traiter et conserver des renseignements personnels (**exemples:** systèmes informatiques, services infonuagiques, copies de sauvegarde, outils de télécommunication, salles et classeurs d'entreposage des dossiers papier).

### Dégager une vue d'ensemble de la circulation des renseignements personnels tout au long de votre projet

À partir des points d'interaction que vous avez identifiés, illustrez le parcours des renseignements personnels tout au long du processus visé par votre projet.

---

[18] Les renseignements biométriques sont des renseignements portant sur les caractéristiques biologiques ou comportementales d'une personne. Ils sont généralement destinés à déterminer son identité (**p. ex.** empreintes digitales, forme du visage, empreinte de l'iris, empreinte de la voix, démarche, signature, renseignements génétiques).

[19] Un identifiant unique est une information qui permet de distinguer un individu dans un ensemble (**p. ex.** un numéro de client ou d'employé).

Cette vue d'ensemble peut être décrite et/ou schématisée. Le schéma est une façon simple et avantageuse de présenter l'information en un coup d'œil.

Cette description ou ce schéma sera plus complexe pour les grands projets, de sorte qu'un découpage par processus pourrait s'avérer préférable.

## Identifier les particularités de chaque phase de votre projet

La **phase de développement** de votre projet peut comporter des risques en matière de vie privée qui sont différents de ceux qui existeront dans la **phase d'exploitation** :

- Phase de **développement** : votre projet prend forme, vous élaborez des solutions pour résoudre les problèmes qui émergent. Des personnes interviennent ponctuellement durant cette phase (par exemple, des consultants). Vous faites des périodes d'essais sur différents produits. Le projet peut être modifié en cours de route.
- Phase d'**exploitation** : votre projet est vivant, vous veillez à ce qu'il produise les résultats escomptés. Des événements peuvent survenir spécifiquement durant cette phase, comme des mises à jour du système. Des employés peuvent quitter votre entreprise. Des personnes peuvent vous faire des demandes d'accès à l'information.

**Exemple 1 :** Je suis directeur commercial d'une entreprise qui fabrique des vêtements sur mesure. J'aimerais proposer un outil de commande en ligne disponible pour mes clients.

Une firme spécialisée sera embauchée durant **la phase de développement**. Je dois prévoir que ces consultants entreront en contact avec certains renseignements concernant mes vendeurs et mes clients tout au long de la mise en place du système. Cependant, ils n'y auront plus accès un certain temps après la mise en service du système, lors de la **phase d'exploitation**. De plus, je dois considérer que les risques de bogues informatiques seront plus élevés durant cette période. Que dois-je prévoir pour réduire les risques?

**Exemple 2 :** Je suis directrice des ressources humaines d'une grande organisation gouvernementale. Je vais faire changer le logiciel de gestion des ressources humaines. Le fournisseur du logiciel m'avise que le système est mis à jour fréquemment et m'informe que des refontes plus importantes sont à prévoir dans la prochaine année. Je dois anticiper ces éventuelles refontes qui arriveront en **phase d'exploitation**. Je dois mettre des moyens en place afin que ces opérations de maintenance n'aient pas d'incidence sur les données personnelles des employés.

### À COMPLÉTER

- Inventaire des renseignements personnels impliqués
- Vue d'ensemble de la circulation des renseignements

# 2. ANALYSER ET ÉVALUER LES FACTEURS RELATIFS À LA VIE PRIVÉE

Cette étape est l'essence de la démarche. Il s'agit de considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées.

**Ces facteurs sont :**

- La conformité de votre projet à la législation applicable à la protection des renseignements personnels et le respect des principes qui l'appuient;
- L'identification des risques d'atteinte à la vie privée engendrés par votre projet et l'évaluation de leurs impacts;
- La mise en place de stratégies pour éviter ces risques ou les réduire efficacement.

## 2.1. Respecter les obligations et les principes de protection des renseignements personnels

**Posez-vous les questions suivantes :**

- Respectez-vous les obligations et les principes de protection des renseignements personnels pour chacune des catégories de renseignements personnels, à chacun des points d'interaction et tout au long du cycle de vie des renseignements?
- Sinon, quelles sont les modifications que vous devriez apporter à votre projet pour que vos obligations et les principes soient respectés?

Documentez les moyens qui sont mis en place pour respecter vos obligations et ces différents principes.

En cas de doute concernant le respect de vos obligations légales, **n'hésitez pas à consulter un juriste**.

Pour **les entreprises du secteur privé**, les principes applicables sont les suivants :

- **Déterminer les fins de la collecte :** Vous devez avoir un intérêt sérieux et légitime pour constituer un dossier sur une personne.
- **Limiter la collecte de renseignements personnels :** Vous devez collecter uniquement les renseignements nécessaires pour offrir votre bien ou votre

service. Votre collecte doit se faire par des moyens licites. Sauf exception, la collecte doit se faire auprès de la personne concernée.

- **Informer la personne concernée :** Avant de constituer un dossier, vous devez informer la personne concernée des finalités du dossier, de l'utilisation qui sera faite des renseignements personnels, des catégories de personnes qui y auront accès au sein de votre entreprise et de l'endroit où ils seront détenus. Vous devez également informer les personnes concernées des droits d'accès et de rectification qui leur sont accordés par la Loi sur le privé. Vous devez inscrire quel est l'objet du dossier.
- **Mettre en place des mesures de sécurité appropriées :** Vous devez prendre les mesures de sécurité propre à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits. Ces mesures doivent être raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.
- **Limiter l'accès aux renseignements personnels :** Limiter l'accès aux renseignements personnels aux seules personnes ayant la qualité pour le recevoir au sein de l'entreprise lorsque ce renseignement est nécessaire à l'exercice de leurs fonctions.
- **Limiter l'utilisation de renseignements personnels :** Vous devez obtenir le consentement de la personne concernée pour utiliser ses renseignements une fois l'objet du dossier accompli, à moins d'une exception prévue par la loi.
- **Obtenir le consentement à communiquer des renseignements personnels :** Vous devez obtenir le consentement de la personne concernée pour communiquer ses renseignements à autrui, à moins d'une exception prévue par la Loi sur le privé;
- **Requérir le consentement des personnes concernées :** À moins d'une exception prévue par la Loi sur le privé, vous devez obtenir le consentement de la personne concernée avant de collecter auprès d'un tiers, d'utiliser ou de communiquer des renseignements personnels. Ce consentement doit être manifeste, libre, éclairé et être donné à des fins spécifiques. De plus, il ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles vous l'avez demandé.
- **Assurer la qualité des renseignements personnels :** Vous devez veiller à ce que les renseignements personnels que vous détenez soient à jour et exacts au moment où vous les utilisez pour prendre une décision relative à la personne concernée.

- **Permettre l'exercice des droits d'accès et de rectification :** Un renseignement personnel doit pouvoir être accessible et rectifié par la personne concernée.
- **Répondre avec diligence :** Vous devez répondre avec diligence aux demandes d'accès aux renseignements personnels et de rectification soumises par les personnes concernées.

**Pour les organisations du secteur public, les principes applicables sont les suivants :**

- **Assumer vos responsabilités** : Chaque organisme public a la responsabilité d'assurer le caractère confidentiel des renseignements personnels qu'il détient.
- **Déterminer les fins de la collecte de renseignements personnels :** Avant d'entreprendre toute collecte d'information, vous devez définir les raisons pour lesquelles vous comptez recueillir et utiliser un renseignement personnel.
- **Limiter la collecte de renseignements personnels :** Vous ne pouvez recueillir que les seuls renseignements personnels nécessaires à l'exercice des attributions de votre organisme ou à la mise en œuvre d'un programme dont il a la gestion.
- **Informer la personne concernée :** Vous avez l'obligation d'informer adéquatement la personne concernée avant qu'elle vous fournisse les renseignements personnels attendus.
- **Limiter l'accès aux renseignements personnels :** La Loi sur l'accès prévoit qu'un renseignement personnel ne sera accessible qu'aux seules personnes ayant la qualité pour le recevoir au sein d'un organisme public lorsque ce renseignement est nécessaire à l'exercice de leurs fonctions.
- **Requérir le consentement des personnes concernées** : Un renseignement personnel demeure inaccessible tant que la personne concernée n'a pas consenti à sa divulgation[20].
- **Assurer la qualité des renseignements personnels :** Un renseignement personnel doit être maintenu à jour, être exact et complet afin de servir adéquatement aux fins pour lesquelles il a été recueilli ou est utilisé.

[20] Certaines exceptions précisées par la Loi sur l'accès autorisent la communication de renseignements personnels sans le consentement préalable des personnes concernées.

- **Mettre en place des mesures de sécurité appropriées :** Vous devez prendre les mesures de sécurité propre à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits. Ces mesures doivent être raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.
- **Permettre l'exercice des droits d'accès et de rectification :** Un renseignement personnel doit pouvoir être accessible et rectifié par la personne concernée.
- **Limiter la durée de conservation des renseignements personnels :** Vous êtes tenus de détruire irréversiblement tout renseignement personnel lorsque l'objet pour lequel il a été recueilli est accompli.
- **Répondre dans les délais légaux :** Vous devez répondre aux demandes d'accès aux renseignements personnels et de rectification soumises par les personnes concernées dans les vingt jours suivant leur réception.

## 2.2. Repérer et décrire les risques sur la vie privée engendrés par votre projet

**Qu'est-ce qu'un risque?** Il s'agit d'une situation ou d'un évènement futur qui peut ou non se réaliser et qui causerait une perte ou un préjudice. Le risque est une *menace potentielle*.

Un **risque sur la vie privée** consiste en un événement qui causerait une perte ou un préjudice à une personne au niveau du respect de son intimité ou de sa vie personnelle.

Dans ce cas-ci, la perte ou le préjudice n'a pas besoin d'être tangible : les effets de l'atteinte à la vie privée peuvent être manifestes et externes (**exemple :** en cas de dommage à la réputation), où être vécues de l'intérieur par les personnes concernées (**exemple** : sentiment d'intrusion).

Dans ce contexte, certains aspects d'un projet qui sont conformes du point de vue légal peuvent quand même être perçus comme une atteinte à la vie privée par les personnes concernées.

### Faire la gestion des risques dans le cadre de l'EFVP

Cela consiste à recenser les risques auxquels votre organisation est exposée, puis à définir et à mettre en place des mesures préventives appropriées en vue de supprimer ou d'en atténuer les conséquences.

Vous devez donc établir des scénarios de tels événements qui pourraient découler de la mise en œuvre de votre projet et d'estimer les impacts potentiels sur la vie privée des personnes concernées par ces événements.

**Posez-vous les questions suivantes :**

- Quels sont les situations ou les événements qui peuvent raisonnablement survenir pour chacun des renseignements personnels, à chacun des points d'interaction, tout au long du cycle de vie des renseignements?
- Quels sont les situations ou les événements qui pourraient engendrer une perte ou un préjudice pour les personnes concernées du point de vue du respect de leur vie privée?

Dressez la liste des réponses que vous donnerez à ces questions et décrivez brièvement ces situations.

**Exemples** de risques sur la vie privée :

- Conservation de renseignements lorsque leur utilité n'est plus démontrée;
- Vol de renseignements personnels;
- Collecte excessive de renseignements;
- Divulgation non autorisée de renseignements personnels;
- Réidentification de renseignements préalablement anonymisés;
- Manque d'information fournie aux individus lors de la collecte;
- Création excessive ou non justifiée d'informations;
- Objectif du projet pas suffisamment important ou non légitime;
- Intrusion dans la vie privée disproportionnée par rapport à l'objectif visé par le projet.

Votre organisation a peut-être déjà en main des avis juridiques ou les résultats d'analyses de sécurité informatique. Si des risques de non-conformité ou des risques en matière de sécurité de l'information ont été abordés dans ces documents, vous pouvez vous en inspirez pour produire votre EFVP.

## Décrire et évaluer les impacts potentiels

Chacun des risques peut causer des impacts qu'il convient de décrire, puis d'évaluer.

Les **impacts potentiels** sont variés :

- vol d'identité et fraudes;
- dangers sur la vie et sur la sécurité des personnes (comme les possibilités de harcèlement);
- pertes financières ou d'opportunités;
- dommage à la réputation;
- sollicitation non désirée; et
- Intrusions et autres nuisances dans la vie privée des personnes.

Les considérations en lien avec les dommages à la réputation de votre organisation, les coûts potentiels que l'événement pourrait vous faire encourir, les litiges qui pourraient s'en suivre ou toute autre conséquence négative portée à votre organisation ne doivent pas entrer en ligne de compte dans votre évaluation des impacts sur la vie privée des personnes concernées.

## Identifier les causes de ces risques

Précisez quelles seraient les causes de ces situations.

Les **causes potentielles** sont également variées :

- un processus déficient;
- des erreurs dans la manipulation des renseignements;
- un manque de connaissances ou de formation;
- des mécanismes de surveillance insuffisants ou inexistants;
- une distribution inadéquate des responsabilités;
- des comportements malveillants;
- une collecte excessive de renseignements;
- des technologies défaillantes ou désuètes;
- l'utilisation non justifiée ou non nécessaire de renseignements sensibles;
- l'absence de consentement;
- l'existence d'un moyen alternatif moins intrusif et suffisamment efficace pour atteindre l'objectif visé.

## Tenez compte de certaines particularités

### Projets impliquant de nouvelles technologies

Certaines technologies soulèvent des enjeux particuliers et les technologies émergentes suscitent des questions parfois inédites.

Pour évaluer adéquatement les risques qu'une technologie comporte, il est essentiel de bien la connaître avant de la déployer, surtout si celle-ci n'a jamais été utilisée auparavant.

L'utilisation de données biométriques est un exemple de technologies qui suscitent des questions et des enjeux particuliers[21].

Demandez l'aide de spécialistes si vous ne pouvez pas effectuer une évaluation adéquate par vous-même.

### Projets d'envergure

Les grands projets génèrent davantage de risques, car ces risques peuvent toucher davantage de personnes.

Pour les projets comportant plusieurs phases, il peut être avantageux ou nécessaire de produire une EFVP pour chacune d'elle. L'environnement et les risques de chacune des phases seront différents.

Pour les projets s'échelonnant sur de longues périodes, une mise à jour régulière de l'EFVP peut être profitable pour le bon déroulement du projet.

### Projets comportant des enjeux éthiques

Certains types de projets exigent qu'une évaluation soit produite par un comité d'éthique. C'est notamment le cas des recherches scientifiques portant sur des humains. Des recommandations en lien avec la protection de la vie privée sont parfois émises par ces comités. Celles-ci devraient normalement être considérées dans vos évaluations.

Des rapports d'évaluation éthique des nouvelles technologies sont fréquemment diffusés par des organismes indépendants ou des chercheurs universitaires. Ces documents abordent bien souvent des questions de vie privée. Ce sont des sources d'information pertinentes pour réfléchir aux enjeux et aux risques générés par les projets technologiques.

---

[21] Pour toute information concernant l'utilisation de systèmes biométriques, veuillez-vous référer au guide produit par la Commission intitulé Biométrie : principes à respecter et obligations légales des organisations. à ce sujet

## 2.3. Évaluer l'impact des risques identifiés

### Se doter d'une méthode pour qualifier les risques

Il n'y a pas de méthode prescrite pour qualifier ou évaluer les risques ni pour présenter les résultats de votre analyse. Néanmoins, une évaluation en fonction de l'impact potentiel d'un événement et de la probabilité qu'il se concrétise peut répondre aux objectifs de l'EFVP.

L'évaluation des risques est un processus subjectif, il est souvent utile de constituer un comité pour tenir cette activité.

Si des pratiques en matière de gestion de risques sont en vigueur dans votre organisation, privilégiez-les.

### Évaluer l'impact de chacun des risques identifiés

L'appréciation de l'impact peut se faire à l'aide d'un système de cotes.

**Exemple** d'un système de cotes pour apprécier **l'impact d'un risque** :

- Très faible et/ou inexistant (1) : le risque n'engendre aucune conséquence pour les personnes, ou des conséquences très mineures pour une seule personne;
- Faible (2) : le risque engendre des conséquences mineures pour une personne ou pour un petit nombre de personnes;
- Grand (3) : le risque engendre des conséquences importantes pour une personne ou des conséquences mineures pour un grand nombre de personnes;
- Très grand (4) : le risque engendre des conséquences majeures pour une personne ou des conséquences importantes pour un grand nombre de personnes;
- Inacceptable (non coté) : le risque engendre des conséquences trop importantes et/ou implique une non-conformité aux lois.

**L'évaluation de l'impact peut être influencée par certaines variables**

- La quantité de renseignements impliqués;
- La nature et la sensibilité des renseignements impliqués;
- La gravité et la nature des préjudices qui pourraient être causés aux personnes (**exemples :** impacts sévères sur la vie personnelle ou professionnelle, sur les

finances, procédures juridiques pour résoudre la situation, mettre en danger la vie de la personne);

- Le nombre de personnes touchées potentiellement ou le profil de ces personnes (**exemples :** enfants, personnes en situation de handicap, immigrants).

### Estimer la probabilité que les risques se réalisent

Votre estimation peut aussi se faire à l'aide d'un système de cotes.

**Exemple** d'un système de cote pour évaluer **les probabilités** :

- Très faible et/ou inexistant (1) : Le risque n'a aucune chance de se concrétiser;
- Faible (2) : le risque a peu de chance de se concrétiser ou un événement similaire ne s'est jamais produit;
- Grand (3) : le risque a de bonnes chances de se réaliser ou un événement similaire s'est déjà produit à une ou quelque reprises;
- Très grand (4) : le risque a de très grandes chances de se concrétiser ou un événement similaire s'est produit à plusieurs reprises

Considérant que le risque zéro n'existe pas, cette estimation peut être très difficile à faire. Soyez réaliste : évitez d'être trop confiant ou trop conservateur.

### Considérer les stratégies et moyens de contrôle existants

Votre organisation peut déjà avoir mis en place des outils, des politiques, des directives, des procédures ou d'autres moyens pour atténuer ou éliminer le risque sans que des mesures supplémentaires n'aient été adoptées.

Listez-les et réévaluez les risques à la lumière de ces informations.

### Déterminer le seuil acceptable de tolérance pour chaque risque

Mettez-vous dans la peau des personnes concernées et demandez-vous comment elles pourraient s'attendre à ce que leurs renseignements personnels soient utilisés et protégés.

Fixez-vous des seuils à atteindre selon ce qui pourrait paraître acceptable pour ces personnes.

Vous devez établir ces seuils en tenant compte du contexte de votre projet. Par exemple, une personne qui fournit des renseignements médicaux a des attentes différentes envers un centre hospitalier qu'envers des publicitaires.

## 2.4. Éliminer ou réduire les risques d'atteintes à la vie privée

### Étudier les stratégies envisageables pour éliminer ou réduire les risques

Les stratégies peuvent chercher à réduire, soit l'impact du risque, soit les chances que ce dernier se concrétise, soit les deux en même temps.

Ainsi, réduire la quantité de renseignements personnels que vous collectez réduit l'impact d'un vol de données. L'ajout de mesures de sécurité réduit plutôt les probabilités qu'il se réalise.

**Exemples** de stratégies :

- Prévoir une révision périodique des différentes collectes de renseignements personnels;
- Mettre en place un système de gestion documentaire qui permet l'application automatisée du calendrier de conservation;
- Revoir les processus d'attribution et de gestion des accès informatiques;
- Engager des firmes de sécurité informatique pour revoir périodiquement les paramètres de sécurité de la prestation électronique de service;
- Revoir les clauses des contrats en matière de confidentialité;
- Établir un calendrier de formation et d'activités de sensibilisation pour vos employés;
- Faire une campagne d'information concernant votre nouvelle utilisation des renseignements personnels;
- Journaliser les accès et exploiter les journaux pour détecter les anomalies;
- Dépersonnaliser ou anonymiser les renseignements si leur utilisation sous une forme nominative n'est pas requise pour tous.

### Choisir les stratégies à adopter

Déterminez quelles stratégies et quels moyens vous mettrez en place pour éliminer ou réduire un risque.

Ce choix ne peut se faire sans tenir compte de la réalité de votre projet et de votre organisation ainsi que des ressources à votre disposition. Songez à des solutions réalisables pour votre organisation.

## Réévaluer le niveau de chacun des risques

À la lumière des stratégies et moyens retenus, réévaluez le niveau d'impact du risque et la probabilité qu'il se concrétise.

Vérifiez si vous avez atteint le seuil de tolérance que vous vous étiez fixé. Si le seuil n'est pas atteint, réévaluez votre choix de stratégies ou de moyens.

Si après avoir revu votre choix, vous ne parvenez toujours pas à éliminer un risque important ou que le seuil de tolérance que vous vous étiez fixé n'est pas atteint*, pensez à revoir en profondeur cet aspect de votre projet ou à le retirer.*

Tout risque qui persiste à la fin, une fois que vous avez pris les mesures visant à diminuer ou éliminer les risques identifiés au départ, devient un **risque résiduel**.

Il est possible que des risques d'atteinte à la vie privée subsistent même après avoir éliminé ou minimisé la plupart d'entre eux. Votre organisation doit néanmoins être en mesure d'assumer la responsabilité des risques résiduels qu'elle fait encourir aux personnes concernées.

**Un conseil**

Même si un risque est complètement éliminé ou qu'une stratégie n'est pas retenue, vous gagnez à garder des traces de votre démarche. Votre organisation pourra ainsi s'y référer dans le futur. Elle pourra connaître les raisons qui vous ont poussé à faire vos choix ou évitera de refaire la démarche complète inutilement.

## Revoir la proportionnalité de votre solution

Après avoir terminé l'exercice de gestion des risques, refaites l'exercice d'évaluer la proportionnalité de votre projet par rapport aux risques qu'il fait toujours encourir aux personnes concernées (voir section 1.2).

À la lumière de l'ensemble de votre évaluation de facteurs relatifs à la vie privée, est-ce que la solution que vous proposez pour atteindre vos objectifs paraît toujours proportionnelle compte tenu de ces risques?

En cas de plaintes par une personne concernée ou de vérification par un organisme de contrôle, serez-vous prêt à démontrer qu'il s'agit d'une solution proportionnelle?

## 2.5. Faire le suivi de l’évaluation des facteurs relatifs à la vie privée

### Établir votre plan d’action

La préparation d’un plan d’action permet d’assurer la mise en œuvre des stratégies et des moyens retenus.

L’insertion des différentes actions dans vos activités régulières concrétise l’EFVP et permet d’en retirer les bénéfices.

### Identifier les responsables de la gestion des risques résiduels

Il est préférable d’identifier des personnes responsables de surveiller l’évolution des risques résiduels. Ces personnes seront aussi responsables de la gestion de l’événement s’il devait se concrétiser.

### Informer vos autorités

Il est important que les hautes autorités de votre organisation soient tenues informées des résultats de l’EFVP. Elles doivent accepter les conclusions de votre analyse et cautionner les risques qui subsistent malgré les moyens déployés pour les atténuer.

**À COMPLÉTER**

- Description des moyens mis en place pour assurer le respect des obligations et des principes de protection des renseignements personnels
- Évaluation des risques
- Plan d’action

# 3. RÉDIGER UN RAPPORT D'ÉVALUATION

Le rapport est la dernière étape de votre processus de réflexion. Il devrait être simple et accessible : tout lecteur qui n'aurait pas été directement impliqué dans votre projet devrait pouvoir comprendre quel est le projet, comment ce projet est susceptible d'affecter la vie privée et comment vous avez considéré et mesuré les risques identifiés.

## 3.1. À quoi sert le rapport?

Un rapport d'EFVP sert **à consolider** les résultats de votre évaluation. Il permet d'attester de vos démarches et de votre réflexion dans le cas d'une vérification, d'une inspection ou d'une enquête par une autorité réglementaire.

Un **résumé** de votre rapport peut également être diffusé auprès de vos clients, de vos partenaires, de toute autre entité concernée, ou même au sein de votre organisation. Vous pouvez rendre ce résumé public en le publiant sur votre site Web. Le diffuser permet de :

- Faire preuve de transparence auprès des personnes qui font affaire avec votre organisation;
- Démontrer que vous avez pris en considération le respect de la vie privée dans l'élaboration et la mise en œuvre de votre projet.

## 3.2. Rédiger un rapport est-il obligatoire?

**Non**, sauf pour les organismes publics, dans certains cas précis prévus par la Loi sur l'accès. Faire une EFVP est alors obligatoire et requiert la rédaction et la diffusion d'un rapport.

**Exemples** de projets où une EFVP est exigée :

- Projets gouvernementaux visés par la Loi favorisant la transformation numérique de l'administration publique;
- Projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui recueille, utilise, conserve, communique ou détruit des renseignements personnels en vertu du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (R.L.R.Q chapitre A-2.1, r.2).

Même si vous ne prévoyez pas faire de rapport, documenter votre EFVP au fur et à mesure vous permet de conserver une trace écrite de votre démarche. Si vous décidez finalement de rédiger un rapport, l'essentiel du travail aura été fait.

Garder une trace écrite est donc une bonne pratique, répandue dans plusieurs provinces canadiennes[22] et dans plusieurs pays[23].

## 3.3. Que devrait contenir le rapport?

### L'essentiel de votre projet et le cadre dans lequel il s'inscrit

- La description de votre projet;
- Ce qui l'a motivé et les objectifs poursuivis;
- Toutes les parties prenantes au projet, en incluant la description de leur rôle et de leurs responsabilités : celles impliquées dans sa mise en œuvre et celles impliquées par la suite, c'est-à-dire les ressources de votre organisation, vos différents partenaires et votre clientèle;
- Les personnes ou secteurs de votre organisation qui seront responsables de gérer les risques résiduels[24];
- L'inventaire et la vue d'ensemble de la circulation des renseignements personnels impliqués;
- La description des moyens mis en place pour assurer le respect des obligations et des principes de protection des renseignements personnels
- La liste des risques identifiés;
- Vos stratégies, mécanismes et mesures de sécurité déployés pour éliminer ou réduire ces risques;
- Les personnes responsables de mettre en œuvre ces stratégies, mécanismes et mesures de sécurité;
- Un échéancier avec les mesures mises en place pour réévaluer périodiquement (**exemple** : un audit).

[22] En Alberta, par exemple, un rapport d'EFVP est obligatoire pour tout projet en matière de santé. (https://www.oipc.ab.ca/action-items/privacy-impact-assessments.aspx).
[23] En Europe, une analyse d'impact relative à la protection des données (AIPD) est obligatoire quand le traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées ».

### Une mention de l'approbation de votre rapport par les hautes instances de votre organisation

Autrement dit, les détails de l'approbation du rapport, incluant les noms, les postes et les signatures des personnes l'ayant approuvé.

### Des informations complémentaires sous forme d'annexes

- Une liste de vos politiques pertinentes en matière de gestion des renseignements personnels et de protection de la vie privée;
- Résumé des avis de sécurité produits en collaboration avec des fournisseurs ou partenaires (**exemple** : test d'intrusion);
- Certifications obtenues dans le cadre de votre projet (quand un organisme d'évaluation certifie que votre produit ou service est conforme à certaines exigences).

**À COMPLÉTER**

- Rapport d'EFVP